どうする？サイバー戦争の放棄!—ロシア・ウクライナ戦争を教訓に

小倉利丸
JCA-NET
2023/4/23

NATOとサイバー軍事演習に参加する日本

日本は、ここ3年間NATOの「ロックド・シールズ」と呼ばれるサイバー戦争の演習に正式に参加している

防衛省
ＮＡＴＯサイバー防衛協力センターによるサイバー防衛演習『ロックド・シールズ２０２３』への参加について

NATOのサイトの告知の日本語訳

参加組織の構成

- 自衛隊の各部隊
- 政府省庁：内閣官房内閣サイバーセキュリティセンター（ＮＩＳＣ）、総務省、警察庁、情報処理推進機構（ＩＰＡ）、ＪＰＣＥＲＴコーディネーションセンター（ＪＰＣＥＲＴ／ＣＣ）
- 「重要インフラ事業者等」として民間からの参加

NATOとサイバー軍事演習に参加する日本

NTT広報

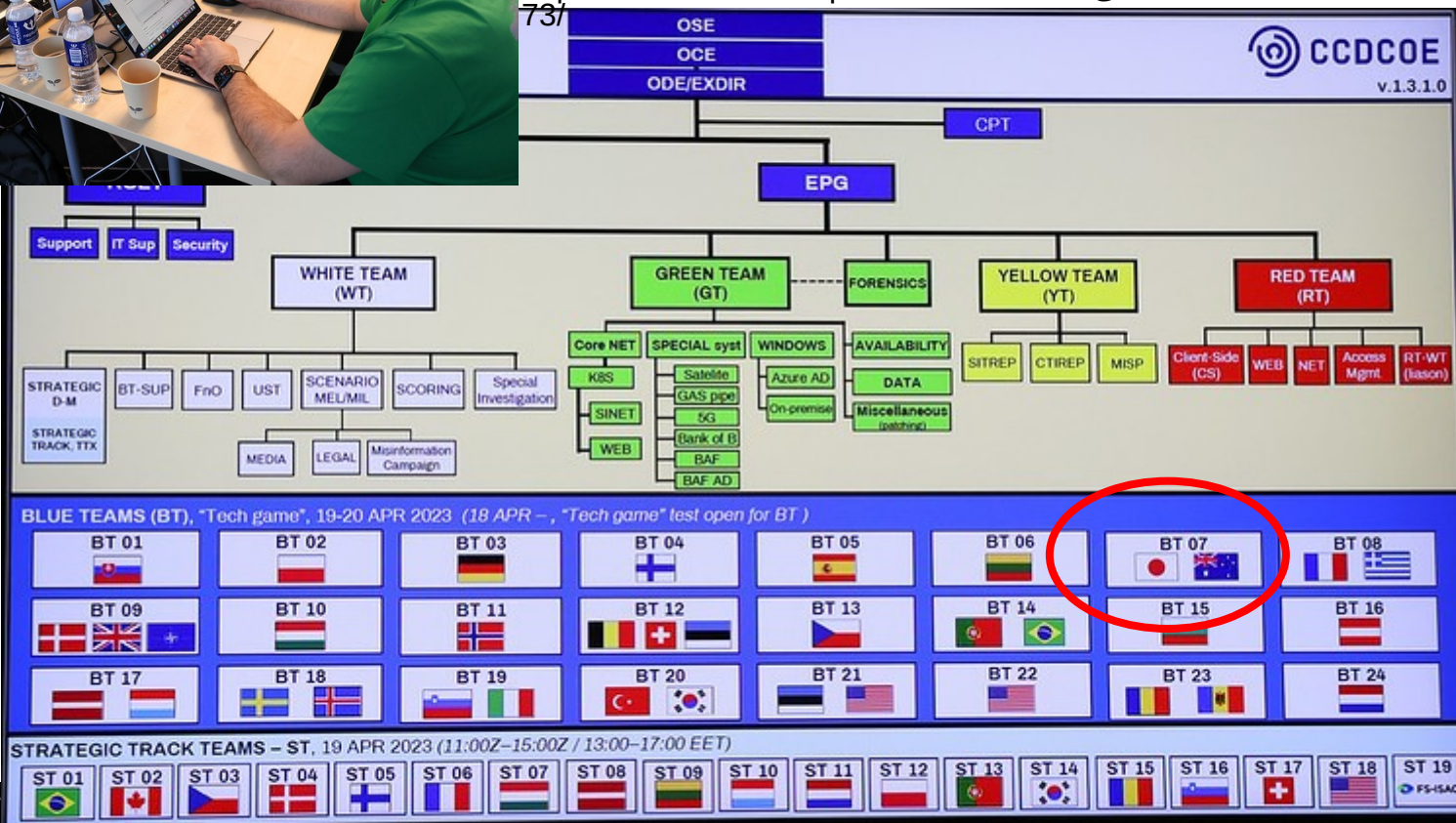
国際サイバー防衛演習「Locked Shields 2023」にNTTグループが参加

「NTTグループは、4月18日から21日まで開催される、NATOサイバー防衛協力センター（CCDCOE: Cooperative Cyber Defence Centre of Excellence）主催の国際サイバー防衛演習「Locked Shields 2023」に参加します。

NTTドコモ、NTTコミュニケーションズ、NTTデータ、ならびにNTTセキュリティ・ジャパンにとって、今回は昨年に引き続き、2度目の参加になります。本演習は、約40か国が参加し、架空の国に対するサイバー攻撃を想定して行われるものです。

　日本チームは、同志国や団体との連携を深め、サイバーインシデント対応能力を共同で強化するため、今回は、オーストラリアとチームを組み、日本の政府機関や民間企業、オーストラリア国防省とともに参加します。」

日本はオーストラリアとチームを組む。
日豪のロックシールドでのチーム結成については、昨年12の第１０回日豪外務・防衛閣僚協議（「２＋２」）共同声明でも言及された。

出典
https://www.flickr.com/photos/133800821@N02/albums/72177720307610786/with/52829377973/

NATOとサイバー軍事演習に参加する日本

NTTのほかにも幾つも企業が参加している。政府関連の機関のJPCERTは毎年参加レポートを公開している。

https://blogs.jpcert.or.jp/ja/2022/05/locked-shields-2022.html

サイバー戦では、私たちの通信環境に身近な組織や企業が大挙参加している。

現在、ロシア・ウクライナ戦争ではウクライナの「IT軍」の動向に関心が集まっている。IT軍は、10万から20万のメンバーを世界中から集めており、日本からの参加者もいる。パソコン1台あればサイバー攻撃の当事者になれるというハードルの低さがあり、自分がやっていることの結果を自覚しづらいことも問題だ。

こうした事態と9条のような伝統的な戦争を前提にした戦争概念との乖離がいちじるしい状況になっている。

以下ではウクライナのIT軍の現状を中心に私たちにとっての課題を考える。

憲法9条

国権の発動たる戦争と、武力による威嚇又は武力の行使は、国際紛争を解決する手段としては、永久にこれを放棄する。

②　前項の目的を達するため、陸海空軍その他の戦力は、これを保持しない。国の交戦権は、これを認めない。

憲法9条

「サイバー戦争」では以下の概念はどのように当て嵌まるのだろうか？

- 国権の発動としての戦争
- 武力による威嚇
- 武力の行使
- 陸海空軍その他の戦力
- 国の交戦権

問題提起の構成

- ロシア-ウクライナ戦争における「サイバー戦争」とはどのような事態なのか(具体例)
- ウクライナの「サイバー軍」とは
- 「サイバー戦争」の特徴と問題点
- サイバー戦争放棄のために必要な条件とは
- 9条の限界？
- 私たちのできること？

「サイバー戦争」とは(具体例)

(NHK)あなたはなぜ「参戦」するのか？ウクライナ侵攻でサイバー攻撃に手を染める市民たち

日本から「参戦」した人物

ウクライナの副首相のＩＴ軍の呼びかけは、世界中に発せられた“檄（げき）”だと感じたんです。戦争が早く終わるために、自分たちがやることで、少しでも戦争にストップがかかることに意義があればいいなと思いました

長年、ＩＴエンジニアをしているという男性は、コンピューターの知識はあったものの、これまでサイバー攻撃の経験はなかったという。攻撃手法については独自に情報収集を進めた。インターネット上で公開されているツールを組み合わせることで、すぐに攻撃に参加することができるようになったという。

「サイバー戦争」とは(具体例)

(NHK)あなたはなぜ「参戦」するのか？ウクライナ侵攻でサイバー攻撃に手を染める市民たち

日本から「参戦」した人物

犯罪だという自覚はもちろんあります。ですから葛藤がありました。でもこれはもう、やらなければいけないことだと言い聞かせて続けています。攻撃した先のサイトの関係者、利用者がどれだけ困っているかイメージできますから、当初は、相当精神的に不安定になりました。手が冷たくなったり、体に震えが来たり、そんな状態が１週間くらい続きました。やっている行為自体は、キーボードを打っている、普段の仕事と変わりませんが、“戦争に参加している”という精神的なプレッシャーが大きかったです

男性は、毎日午後、「ＩＴ軍」がＳＮＳ上に投稿する攻撃先リストを確認し、それに基づき、１０ほどのウェブサイトなどに攻撃を行うよう、自身で組んだプログラムを動かすことを繰り返している。そして、男性は、今、当初抱えていた葛藤は薄れてしまっていると話した。

「サイバー戦争」とは(具体例)

(BBC)ウクライナのサイバー最前線で活躍するハッカー軍団を紹介

「ウクライナIT軍」（約20万人のTelegramグループを持つボランティア・ハッキング・ネットワーク）で最も著名なハッカーの一人、オレクサンドルさん。

- ロシアで生産されるすべての商品（生鮮食品も含む）は、工場で作られた瞬間から販売されるまで、その会社が提供する固有の番号とバーコードをスキャンして流通を管理するシステムを標的型DDoS（Distributed Denial of Service）攻撃を使ってシャットダウンさせた。
- ロシアのラジオ局を乗っ取り、偽の空襲サイレンの音と市民に避難を呼びかける警告メッセージを放送した。

IT Stand for Ukraineのローマンさん。

Russia-Ukraine war

By Joe Tidy
Cyber correspondent

When Russia initiated its full-scale invasion of Ukraine, a second, less visible battle in cyberspace got under way. The BBC's cyber correspondent Joe Tidy travelled to Ukraine to speak to those fighting the cyber war, and found the conflict has blurred the lines between those working for the military and the unofficial activist hackers.

When I went to visit Oleksandr in his one-bedroom flat in central Ukraine, I found a typically spartan set-up common to many hackers.

「サイバー戦争」とは(具体例)

(BBC)ウクライナのサイバー最前線で活躍するハッカー軍団を紹介

ウクライナの副首相兼デジタル変革担当大臣であるMykhailo Fedorov

- ウクライナには「市民の命を守るためにできることはすべて行うという道徳的な権利」があると確信している
- 「本格的な戦争の1年間で、ウクライナのハッカーは、そのような侵略にもかかわらず、十分に倫理的に活動していることを示したと思います - そして、戦争に関与しているロシア連邦のもの以外の対象に対して過度の損害を与えることはありません」

「サイバー戦争」とは(具体例)

(BBC)ウクライナのサイバー最前線で活躍するハッカー軍団を紹介

ロシアのハッカー集団Killnetは、ロシア軍のサイバー部門と直接協力

- ウクライナと同盟国の両方の病院のウェブサイトに対する破壊的な攻撃（一時的ではあるが）を呼びかけ、実行
- NATO加盟国のウェブサイトを一時的に混乱させる攻撃を次々と行った

「どこにいても、ノートパソコンと必要なものはすべて手元にある。これによって、私は機動的かつ効率的に、ほとんどすべての時間を我々の運動に捧げることができるのです。」

ウクライナの「IT軍」とは

- 資格：ボランティア、非正規軍
- 規模：2022年春頃 25万～30万人(Telegramチャンネル登録数。ただし、登録は誰でもできるので、登録=参加を意味しない) 2023年4月23日現在で185000人とかなり減少
- 募集方法：オンライン登録
- 参加者の居住地：世界各国
- 2つの構成部分（1）民間のロシアのインフラの標的に対する協調的なDDoS攻撃に参加する意思を持つ人たちを動員するグローバルな行動の呼びかけを継続的に行なう（2）複雑なサイバー作戦を実験し実施してきたウクライナの防衛および情報担当者からなる可能性が高い内部チーム
- 開発者、デザイナー、コピーライターなどのスキルをもつ者を集めている。

ウクライナの「IT軍」とは

IT ARMY of Ukraine
185,130 subscribers

Pinned message #3
IT-армія України атакувала Газпром – головний банк кривавого режи

—

We launched a DDoS attack on the Tochka bank in the morning.
They still can't get over it :) Join in!

🔥 611 👍 99 ❤️ 31 61.9K 21:20

37 comments

IT Army of Ukraine UA EN Пошук інструкцій Запропонувати цілі

Доброго вечора, ми з УКРАЇНИ!

IT ARMY OF UKRAINE

It Army Of Ukraine - це спільнота IT-фахівців з усього світу, які об'єдналися після початку повномасштабного вторгнення в Україну з боку росії. Ми найпотужніша спільнота в Україні і можемо утримувати одночасно більше 800 цілей. Фахівці різного рівня створили та продовжують створювати автоматизовані системи атак на інформаційні ресурси та сервіси країни-ворога. На цьому сайті кожен зможе легко знайти інформцію та приєднатися до боротьби навіть не маючи навичок для цього. А чат під будь-яким постом в телеграм-каналі (ось посилання) дозволить Вам задати питання і отримати на них відповіді від спільноти, якщо Вам все ж таки складно розібратися.

НАША МІСІЯ:

IT ARMY наближає перемогу України у війні, виснажуючи економіку країн-агресорів, заважаючи роботі важливих фінансових, інфраструктурних, державних сервісів та діяльності великих платників податків. Ми також блокуємо ворожу медіапропаганду та доносимо правду про війну до їх аудиторії. Ми бажаємо, щоб кожен мешканець країн-агресорів відчував та втомлювався від агресії, яку скоює їх держава.

Приєднуйтесь до боротьби.

Слава Україні!

It Army Of Ukraineは、ロシアによるウクライナへの本格的な侵攻が始まって以来団結してきた世界中のIT専門家のコミュニティです。私たちはウクライナで最も強力なコミュニティであり、一度に800以上を標的にできます。さまざまなレベルの専門家が、敵国の情報リソースとサービスに対する攻撃の自動システムを作成し、作成し続けています。このサイトでは、誰もが簡単に情報を見つけ、そのためのスキルさえなくても戦いに参加することができます。また、電報チャンネル(の投稿の下でチャットすると、リンク)を使用して、理解が難しい場合でも、質問をしたり、コミュニティから回答を得たりできます。(右上のIT軍サイトの解説)

出典：
上
IT軍のウエッブサイトhttps://itarmy.com.ua/
左上
IT軍のTelegram(2023年4月23日)

ウクライナの「IT軍」とは

TO JOIN US YOU NEED TO HAVE

1

Install tools

Install tools to VPS if you can

We applied automatization to our tools to get new or updated targets without your actions.

That's why we are asking to use recommended tools to synchronize our attacks.

Windows Linux Mac

2

Just launch the attack

Actual targets will be pulled up automatically!

How to launch an attack is indicated in the relevant instructions for the selected DDOS utilities.

Share our website:

必要な「武器」は、パソコンにソフトをインストールするような感覚で行なうことができてしまう。上は、サイバー攻撃に必要なツールのダウンロードサイト Windowsl、Linux、Mac別にツールをインストールし、具体的なDDos攻撃のマニュアルの沿って攻撃をする、ということがシンプルに記述されている

ウクライナの「IT軍」とは

ItArmy of Ukraine UA EN Search Instructions Suggest Targets

INSTRUCTIONS TO CONFIGURE DDOS ATTACKS TO ENEMY COUNTRY

Targets are automatically pulled and coordinated from IT Army of Ukraine.

Instructions for recommended VPN services

Every tool has its own benefits so we cannot recommend one of them more than the others. We suggest you to try them all and choose what works best for you.

The only thing we do recommend is to run the attack on cloud virtual server (VPS). This approach doesn't overload your local network and is more efficient since it allows you to run the tool on multiple instances thus having more resources.

Windows Linux Mac

Attention!
Please turn off the antivirus, install and add the DDOS tool to the exclusions folder before restarting the PC.
Our russian foes leveraged antivirus software to consider DDOS potentially unsecured hence blocked.
We guarantee the DDOS tools recommended on our official website does not conclude any harmful components for your cyber security.

Report VirusTotal: UKITA MHDDOS DB1000N DISTRESS UASHIELD

PRIORITY Instruction for MHDDOS | Instruction for db1000n | Instruction for Distress | Instruction for uaShield

UkITA Installer | MHDDoS

UKRAINE IT ARMY INSTALLER FOR WINDOWS (ALL IN ONE - MHDDOS/DB1000N/DISTRESS)

You can contact for help at IT Army of Ukraine Chat.

Download and install - UkITA Installer (https://github.com/OleksandrBlack/ukita_installer)
Visualization of the installation and launch of the attack

UKITA Installer Setup

Welcome to UKITA Installer Setup

Setup will guide you through the installation of UKITA Installer.

It is recommended that you close all other applications before starting Setup. This will make it possible to update relevant system files without having to reboot your computer.

Click Next to continue.

Next > Cancel

Click Next to continue

Windows版のツールインストール画面(上) インストールを解説したビデオもある(右)

ウクライナの「IT軍」とは

- IT軍のサイトから必要な「武器」がすべて入手できる。
- ITのスキルの高さは要求されていない。普通にPCを使える人でも参加可能なように設計されている。
- 使われている「武器」の基本的な仕組みはGithubで公開されている。
- たとえば、mhddos_proxyというツールを使うと以下が自動化されるという。
  - 自動負荷分散で複数のターゲットを同時に攻撃
  - さまざまな攻撃方法を使用し、それらを自動的に切り替え

ウクライナの「IT軍」とは

- 武器は何か。DDos攻撃が中心(目標サイトの機能麻痺)
- 純粋に攻撃的な性質を持ち、意欲的なアマチュア（民間人）と献身的なプロフェッショナル（民間人、軍人、情報機関）を一つの（おそらく）階層的な組織構造に取り込む役割を担っている。
- ウクライナが所有する IT 企業やウクライナ国外にいる個人、ウクライナ在住で欧米企業のために活動するウクライナ人を含むエコシステム。新たなツールの開発、ノウハウの蓄積、新たなターゲットの特定、その他の情報支援機能
- オンライン薬局、銀行、食品配送サービス、小売業者など、ロシアの民間インフラを執拗かつ無差別に標的にしている

ウクライナの「IT軍」とは

- 誰が組織したのか。ウクライナのMykhailo Fedorovデジタル化担当大臣が中心に。

Fedorovは、ウクライナ南東部ザポリージャ地方出身。ザポリージャ国立大学の社会学・経営学部で学ぶ。2015年にSMMSTUDIOというデジタルマーケティングのスタートアップを設立。4年後、国会議員に選出。

2019年ウクライナの公共サービスを完全にデジタル化することを目標にデジタル変革省を設立した際、そのリーダーに抜擢。現在は副首相を兼ねる。

- Fedorovのやってきたこと
  - マイクロソフトやアップルなどの企業にロシアへのサービスを停止させるデジタルキャンペーンの構築した
  - Twitterやその他のソーシャルメディアプラットフォームで、ロシアを貶め、その虐待の疑いを訴えるウクライナのオンラインキャンペーン。
  - 侵攻から数週間以内にIT軍を創設するための陣頭指揮を執る。
  - イーロン・マスクと、ウクライナ軍の通信基幹となる何千ものスターリンク衛星の配備に関する契約を締結

ウクライナの「IT軍」とは

Fedorovが大西洋評議会に寄稿した文章から。DDosだけでなく以下の四つの攻撃をについて説明している。

Tech innovation helps Ukraine even the odds against Russia’s military might By Mykhailo Fedorov

「軍事技術が最善の解決策を提供することは明らかだ。現代の戦争における成功は、1960年代の戦車を何台配備できるか、あるいは歩兵を大砲の餌にする意思があるかではなく、主にデータとテクノロジーに依存している。」

- Army of Drones

「ドローンは、ロシアのウクライナ戦争における最大のゲームチェンジャーとして特筆に値する」

「戦場でのドローンの重要な役割は、戦時中の国内生産ブームに拍車をかけている。この半年で、UAVを製造するウクライナの企業の数は5倍以上に増えた。この拡大は今後も続くだろう。ロシアによる本格的なウクライナ侵略は、世界初のロボット戦争に発展しつつある。ウクライナが勝つためには、あらゆるジャンルのドローンが大量に必要だ。」

- 総合状況認識システム「Delta」、ウクライナ国防省のイノベーションセンターが開発

「軍隊のためのGoogleマップ」とも言えるものだ。航空偵察、衛星画像、ドローン映像など、さまざまなソースからのデータを統合し、NATOの基準に沿った戦場のリアルタイムビューを提供

ウクライナの「IT軍」とは

Tech innovation helps Ukraine even the odds against Russia’s military might By Mykhailo Fedorov

- 市民の戦況レポート

一般市民が敵軍や軍用機器の動きをレポートできる特別なチャットボット。広く使われているDiaアプリに統合されたこのツール。46万人以上のウクライナ人ユーザー。

- 衛星通信

ウクライナの競争力のひとつであり、前線や解放された地域全体に接続を提供するとともに、停電時にも機能する。ロシアの侵略が始まって以来、ウクライナは30,000台以上のスターリンク端末を導入

「軍事テクノロジーを効果的に活用するウクライナは、"第二のイスラエル "になる可能性があると指摘する人もいる。それはお世辞にも褒め言葉とは言えないが、実際にはウクライナは間違いなくさらに大きな可能性を秘めている。今後数年のうちに、ウクライナはトップクラスの軍事技術ソリューションを持つ国になる可能性がある。」

「サイバー戦争」の特徴と問題点

- 特徴
  - 正規軍ではなくボランティア形式をとるが、組織化に軍や政府が関与(正規軍としないことで、国籍を問わず、官民の区別なしに、大量の人員を動員でき、国家の戦争犯罪としての責任を回避しうる手法。今後の戦争のための組織の特徴になりうる)
  - 組織化にTelegramなどネットのツールを使う
  - 「武器」は誰もが保有しているパソコン
  - 「参加」のハードルが極めて低く、事実上誰でも参加できる。倫理観の希薄化。
  - ボーダーレス：どこの国籍の者でも、通常の市民生活をしながら参加可能
  - 主要な標的は「ソフトターゲット」である場合が多い。防御が厳重な軍事施設や政府の重要施設ではなく、セキュリティホールがありうるシステムが狙われ。結果として一般市民への攻撃となる。(無差別の空爆と類似した性格をもつかも)
  - 非軍事企業ともいえるIT企業など民間との連携。従来の軍事産業の概念では把握できない。
  - 多国籍プラットフォーマーなどとの連携。外国企業の関与が可能。

「サイバー戦争」の特徴と問題点

- 結果として
  - 軍事と非軍事の境界があいまいになる

「僕の場合は、今はルーティンワークで攻撃しています。時間が来て指令が来て攻撃、というのを毎日繰り返しています。そういう人間が、世界中に今25万人以上いるんですよ。感覚が麻痺（まひ）してくると言うか…。戦争が馴染んでしまっている、生活の一部になってしまっている」

  - 非戦闘員と戦闘員の区別がつかなくなっている
  - 技術革新が戦争によって方向づけられている(監視、遠距離殺戮技術の突出)
  - 国際人道法の枠組が機能できなくなっている(国際赤十字が危惧)

サイバー戦争放棄に必要な条件とは

- 従来の「戦争」「平和」の概念をリセットして再定義が必要
- 戦車、戦闘機、軍事基地など可視的で範囲や概念が明確な武力、武器に該当しないが「武器」となるツールが私たちの身近にあり、容易に利用可能である。
- ゲームやフィクションの世界との感覚的な違いがわかりづらい。自分の行動が人間の生存を脅かすような結果をまねいたという実感を持ちにくい。倫理観による歯止めがかかりにくい。
- コンピュータに関連する「平和教育」が必要。学校だけでなく、社会人に対しても必要。しかし、戦争に加担する政府が行なう学校教育に期待できない。オルタナティブが必要になる。
- 企業や研究機関が戦争に加担しないようにする取り組みが、従来の「軍事研究」「軍事産業」の概念では不十分になっている。
- 戦争放棄と経済制裁の関係についての議論とも共通したところがあるのではないか。

9条の限界？

「サイバー戦争」では以下の概念はどのように当て嵌まるのだろうか？定義を明確にすることが必要

国権の発動としての戦争に、ボランティアによる「サイバー戦争」は該当するのか？あるいは、武力による威嚇という場合でも、「サイバー」では何が武力で何が威嚇なのか？などわかりにくいし、反戦平和運動のなかで共通の理解ができていない。

「サイバー領域」における攻撃は、経済制裁の場合と同様に、実空間での陸海空軍その他の戦力の行使と一体となっている。この「一体」の意味は、経済制裁を実施する国と実際の武力行使をする国とが別々であってもよく、ある種の分業と連携による展開でよい。しかしサイバー攻撃は、経済制裁と違って、国家ではなく個人が自国政府や法律の枠にとらわれずに参加することが容易である。(いわゆる伝統的な義勇軍や傭兵よりもずっとハードルが低い) そのために、「国の交戦権」規定では不十分である。他方で、現行法でもサイバー攻撃は犯罪行為だが、これが事実上機能していない。現在日本からもIT軍に参加する個人がいても、日本での取り締まりは事実上なされておらず、結果として黙認されているといえるかもしれない。(もし日本からロシア側のサイバー部隊に参加するとか、日本が敵国とみなす周辺諸国のサイバー部隊に参加するとなれば、取り締まりの対象になると推測しうるのではないか)

一般的に「違法」とされる行為であっても、国家安全保障上必要であれば適法とされる例外規定が制定されがちであり、すでにロック・シールズ演習に日本の官民組織が参加しているように、違法行為が容認される素地がすでにできあがっている。

私たちのできること？

- インターネットはコミュニケーションの道具であり戦争の道具ではないことをどのように共通の理解にできるだろうか？
- 自分のコンピュータを武器として使わない、ということは、具体的にどのようなことだろうか？
  - 敵意を煽るメッセージを投稿することは？
  - 自国に有利な情報を一方的に拡散することは？
- 攻撃された場合の防衛措置をどうすべきか。国に委ねるのか、私たちで対処するのか、その両方か？
- 敵対的な環境のなかで、インターネットは「敵国」の人々とも繋がれるコミュニケーションの道具であることを忘れてはならない。このことは、戦争状態を終らせるための、これまでになかった「回路」の可能性を示唆していないだろうか？

参考資料

参考資料(翻訳は機械翻訳を最低限修正しただけのものです。あくまで参考としてお読みください。公開の場への転載はご遠慮ください)

- (atlanticcouncil)技術革新でウクライナがロシアの軍事力に打ち勝つ

https://cryptpad.fr/pad/#/2/pad/view/n6b3Yv19okt-SiRNjwemupfj60ctrbMPeFv0p-EYTWA/

- (Hill)ウクライナのミレニアル世代の大臣がロシアとのデジタルな戦いをリードする

https://cryptpad.fr/pad/#/2/pad/view/XCtWZKe1BUNprsBmGc0PROvdDRtuMdm9JEETLbnuL6k/

- (Microsoft)ウクライナを守る：　サイバー戦争からの初期の教訓

https://cryptpad.fr/pad/#/2/pad/view/kSnNoYRCSyFc9sx-SkmO9sAXcF+OSCPjTIojSAwwzNY/

- (Google)戦争の霧：ウクライナ紛争がサイバー脅威の状況をどう変えたか

https://cryptpad.fr/pad/#/2/pad/view/PnxLeaYeUjhnrWwn8e+3oVfG3cPYXwd-czH17m-89fs/

- (NewsWeek)ウクライナはサイバー法の起草に奔走、有志のハッカー軍団を合法化へ

https://cryptpad.fr/pad/#/2/pad/view/BjV0XTb2PHFhukurCkYkFzqoMCuW4aWgXgv54LCWjO8/

参考資料

- (国際赤十字委員会)共通理解に向けて：確立されたIHL原則のサイバー作戦への適用

https://cryptpad.fr/pad/#/2/pad/view/BNuwMQRRHzy1XgD8juNk46By9-DGkPZWKtcAeiAC2vU/

- (BBC)ウクライナのサイバー最前線で活躍するハッカー軍団を紹介

https://cryptpad.fr/pad/#/2/pad/view/4mB+GKGNx-lsIYi4erJgUdtRN3D534YP2IHAAr7lc9I/

- (NATO)世界最大規模のサイバー防衛演習「Locked Shields」がタリンで開幕

https://cryptpad.fr/pad/#/2/pad/view/XJQMWYf3RvG7uEwLpB6Yj9+I75PvvKrDkxsiOudIXXs/

- Stefan Soesant「サイバーディフェンスレポート ウクライナのIT軍団」(再掲)

https://cryptpad.fr/pad/#/2/pad/view/klBMODnEZr8g4BE6k3C81kyCAUIJjovWXhEMg81Lu+w/

- 中谷 和弘『サイバー攻撃の国際法 タリン・マニュアル２．０の解説』信山社、2018(The NATO Cooperative Cyber Defence Centreによるマニュアル。現在はバージョン3が出ている)